

Figure 1

2/28
POK 92000 2088 US 1

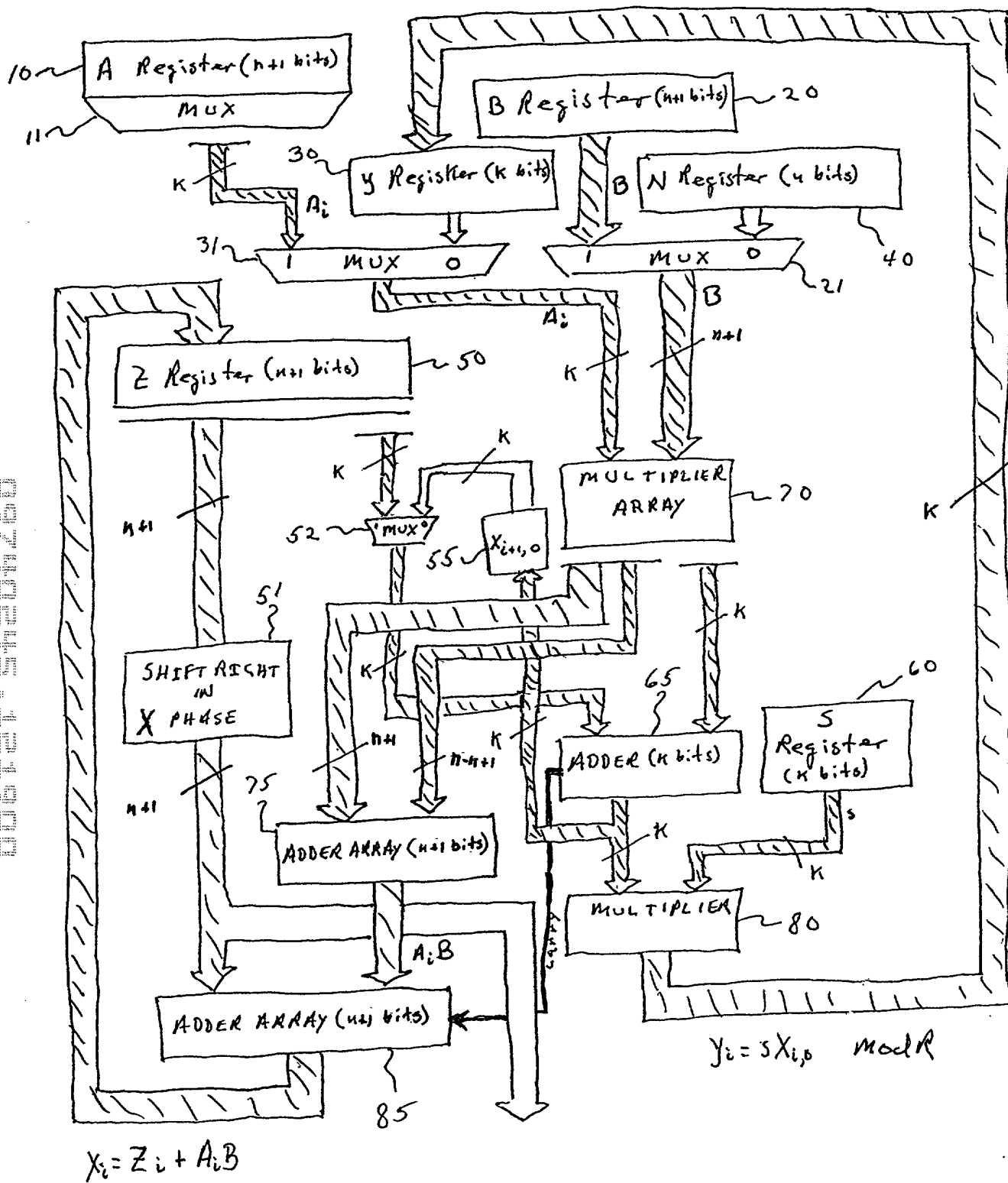


Figure 2

3/28

POL92000 0088451

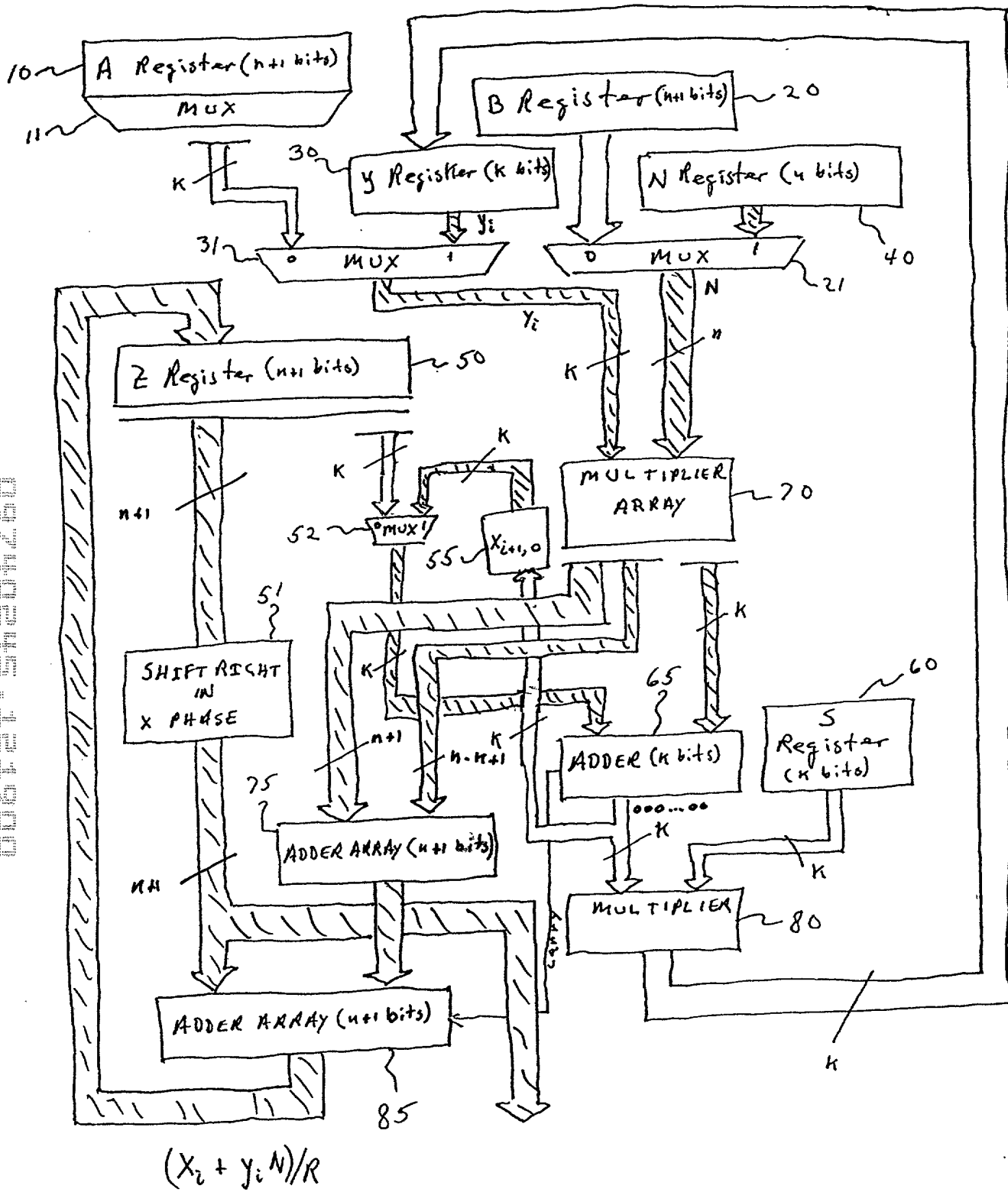


Figure 3

4/28

Pou 92000 0088451

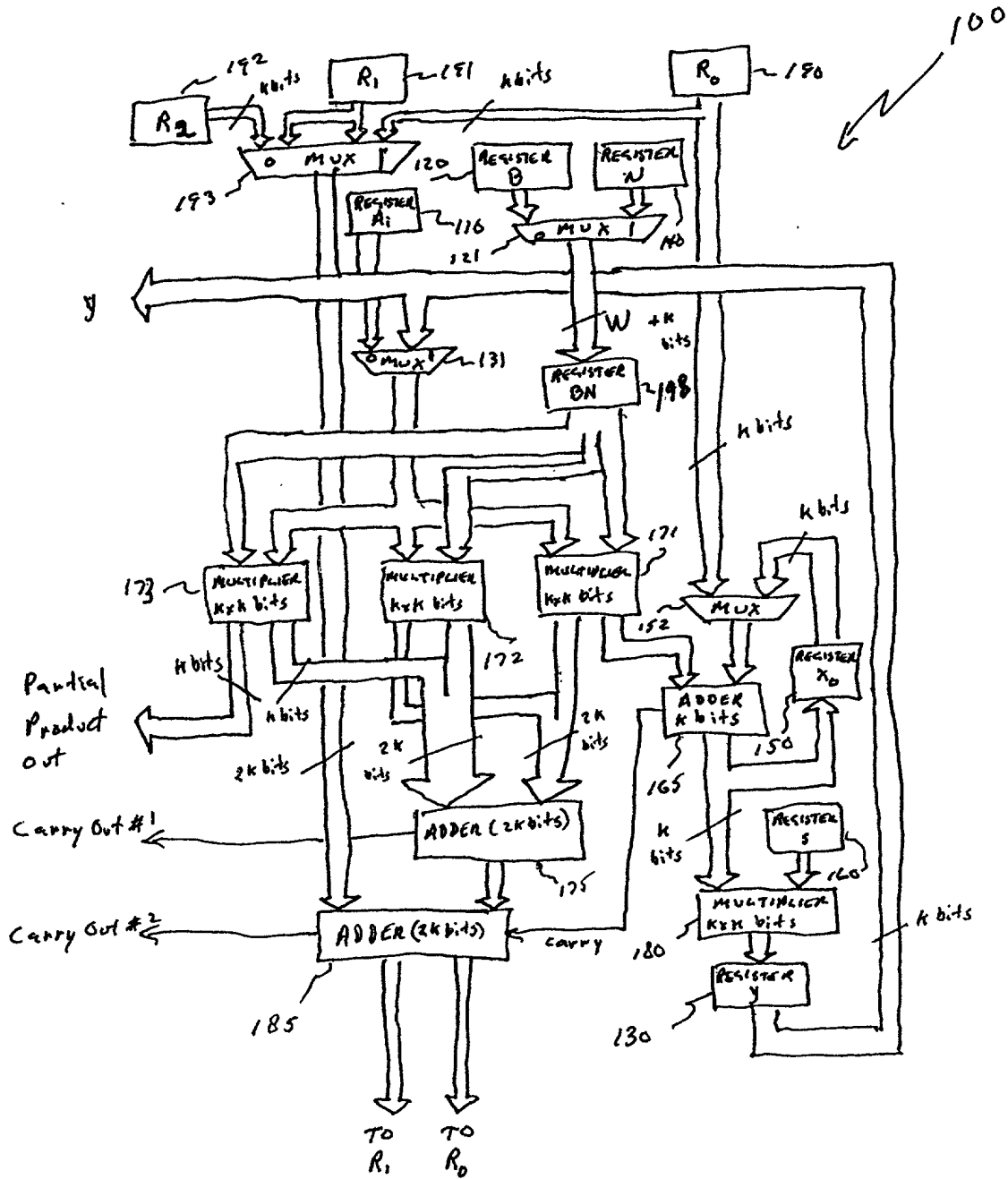


Figure 4

6/28

P0492000 v088us1

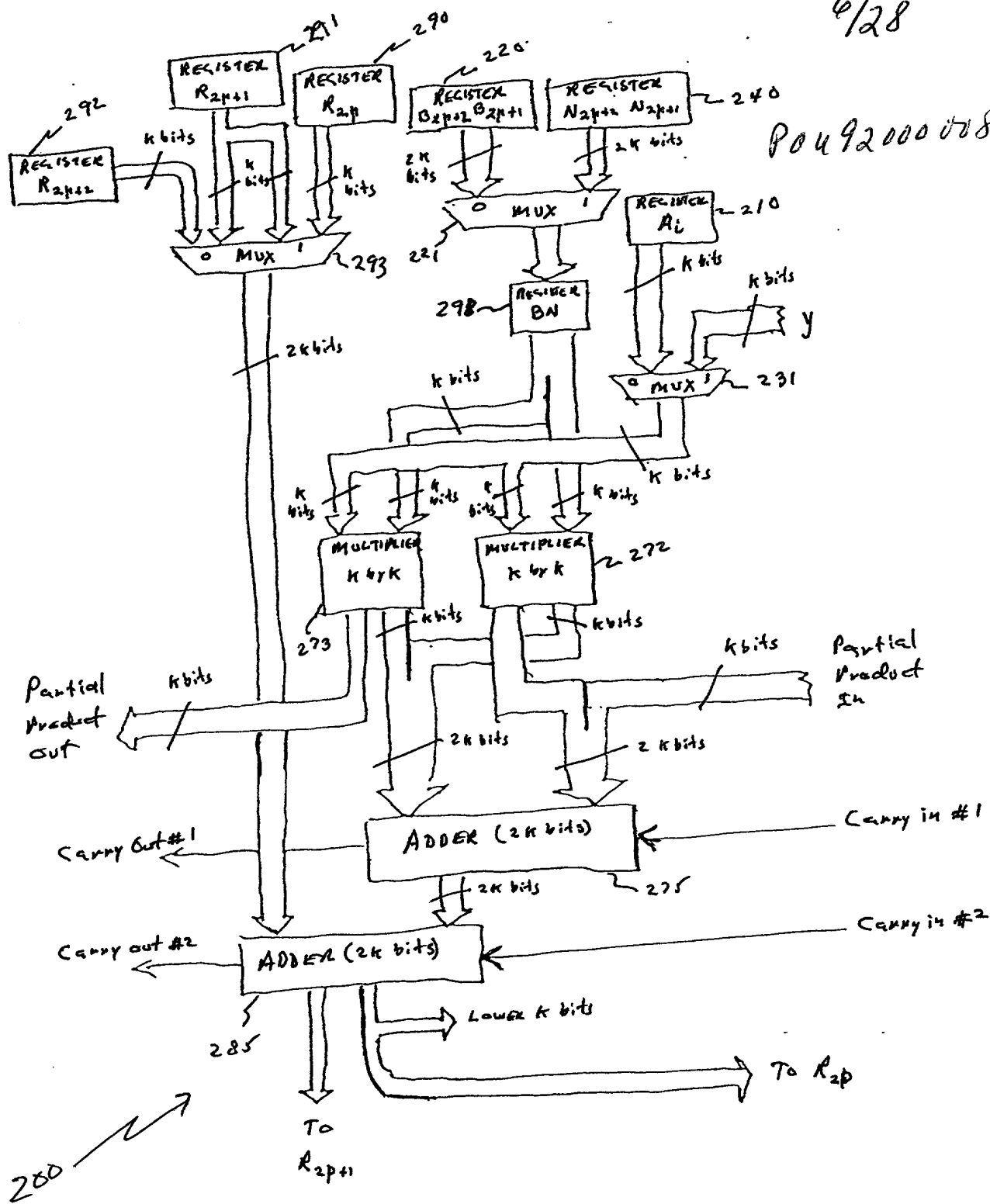


Figure 5

7/28

POU92000088451

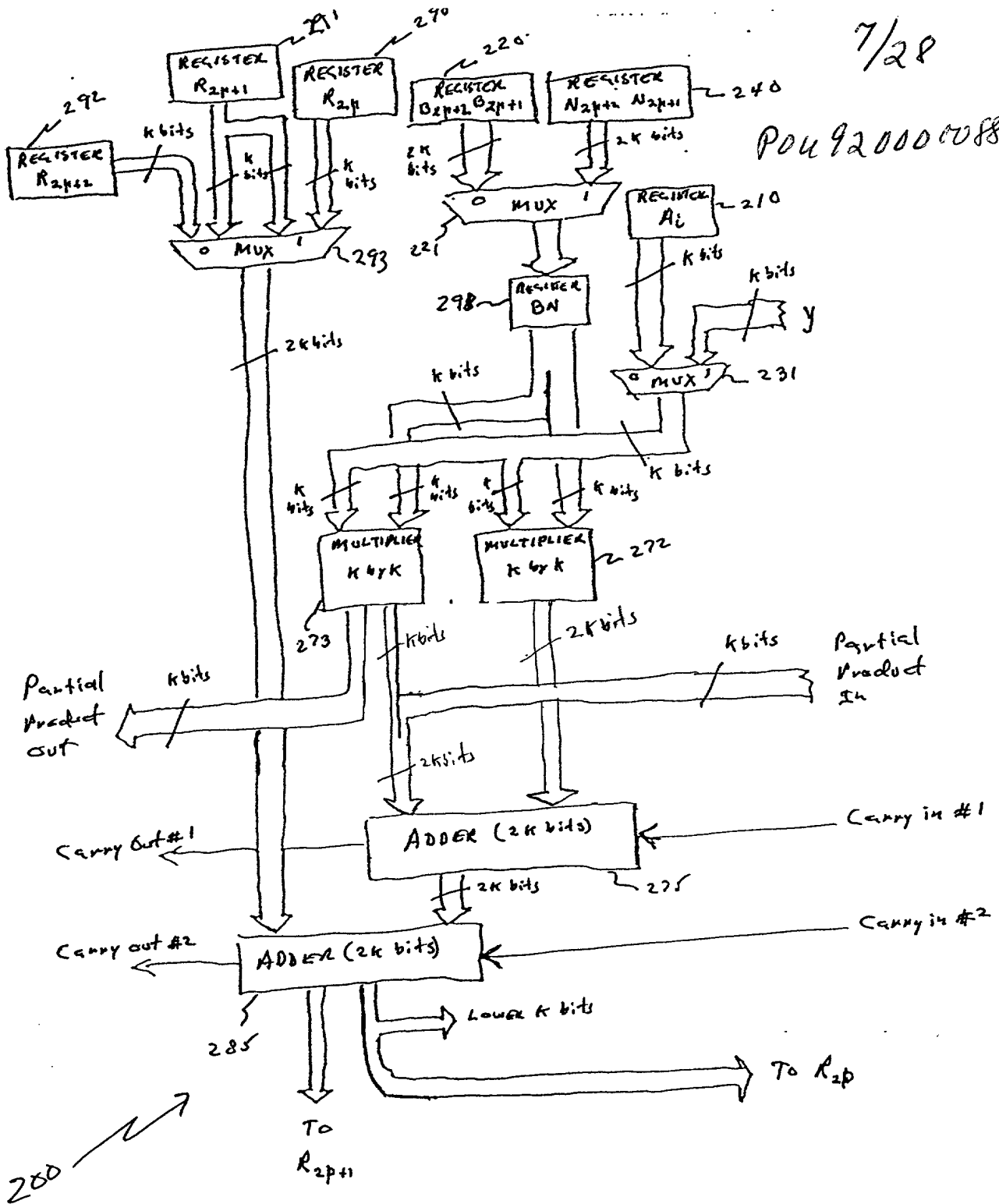


Figure 5A

8/28

POU 920000088451

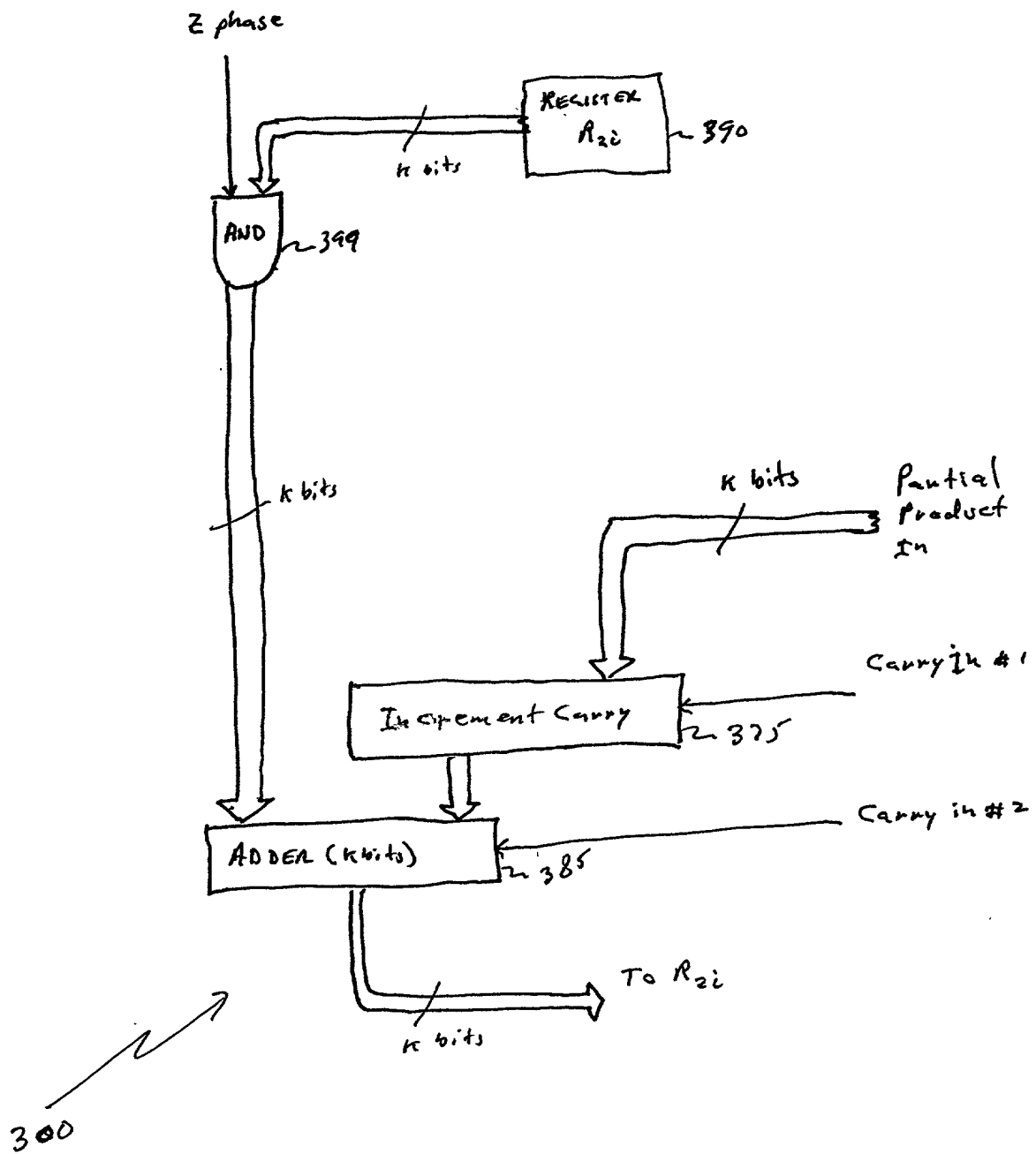


Figure 6

Page 9200 to 9201

9/28

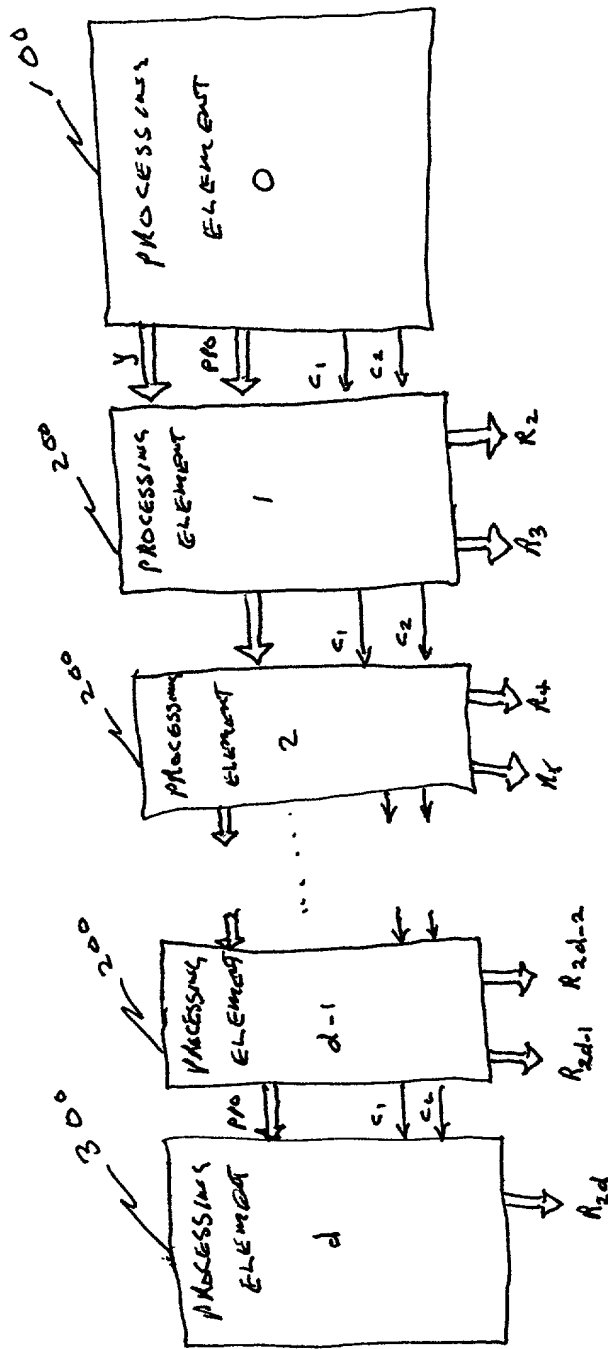


Figure 2

10/28
 For 92000 address

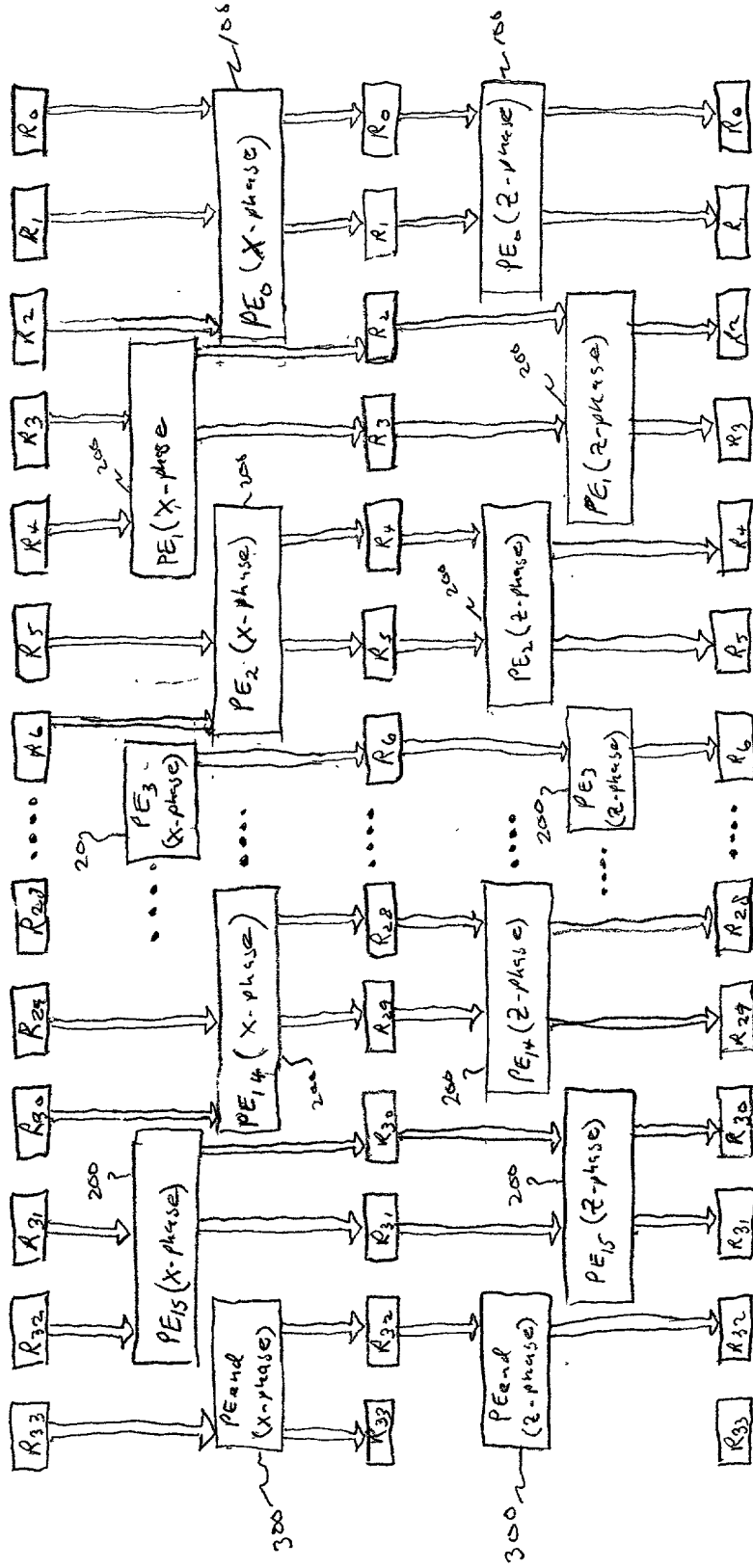


Figure 8

11/28

P0492000 008451

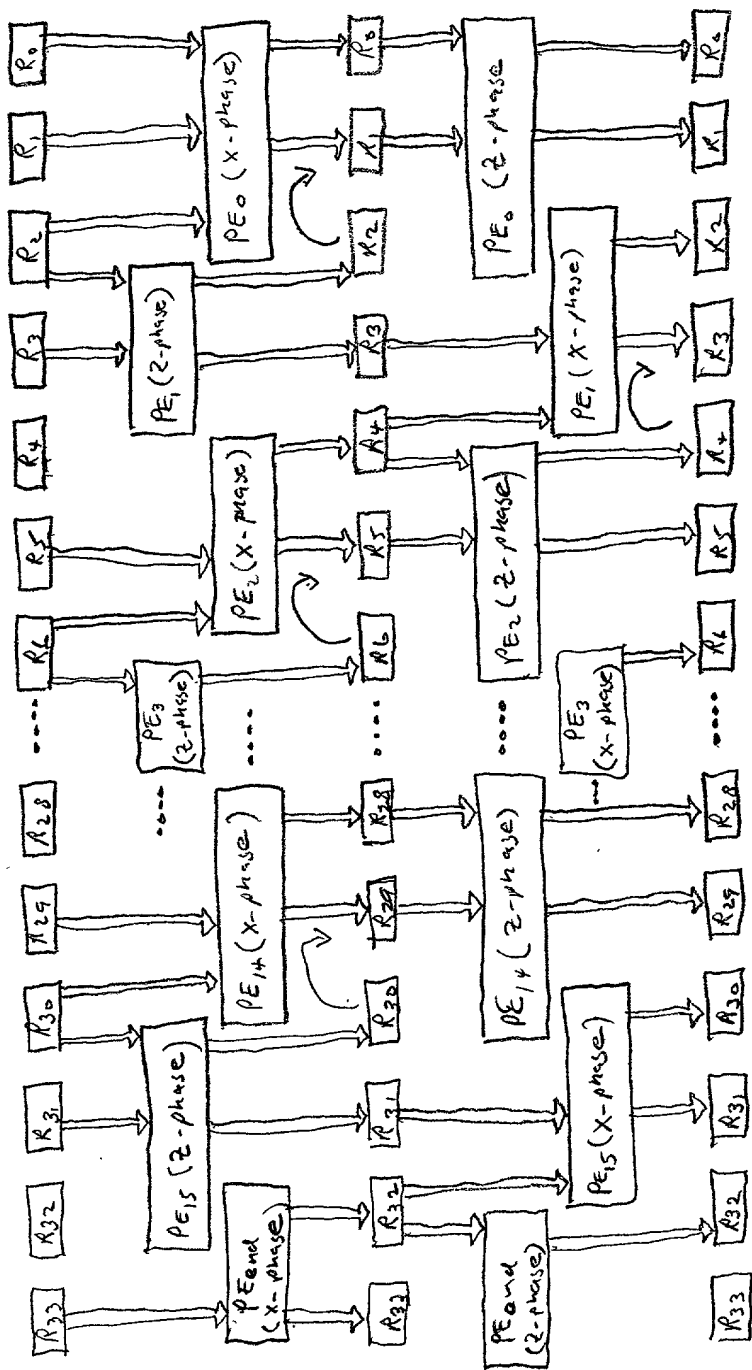


Figure 9

12/28

P04920000088451

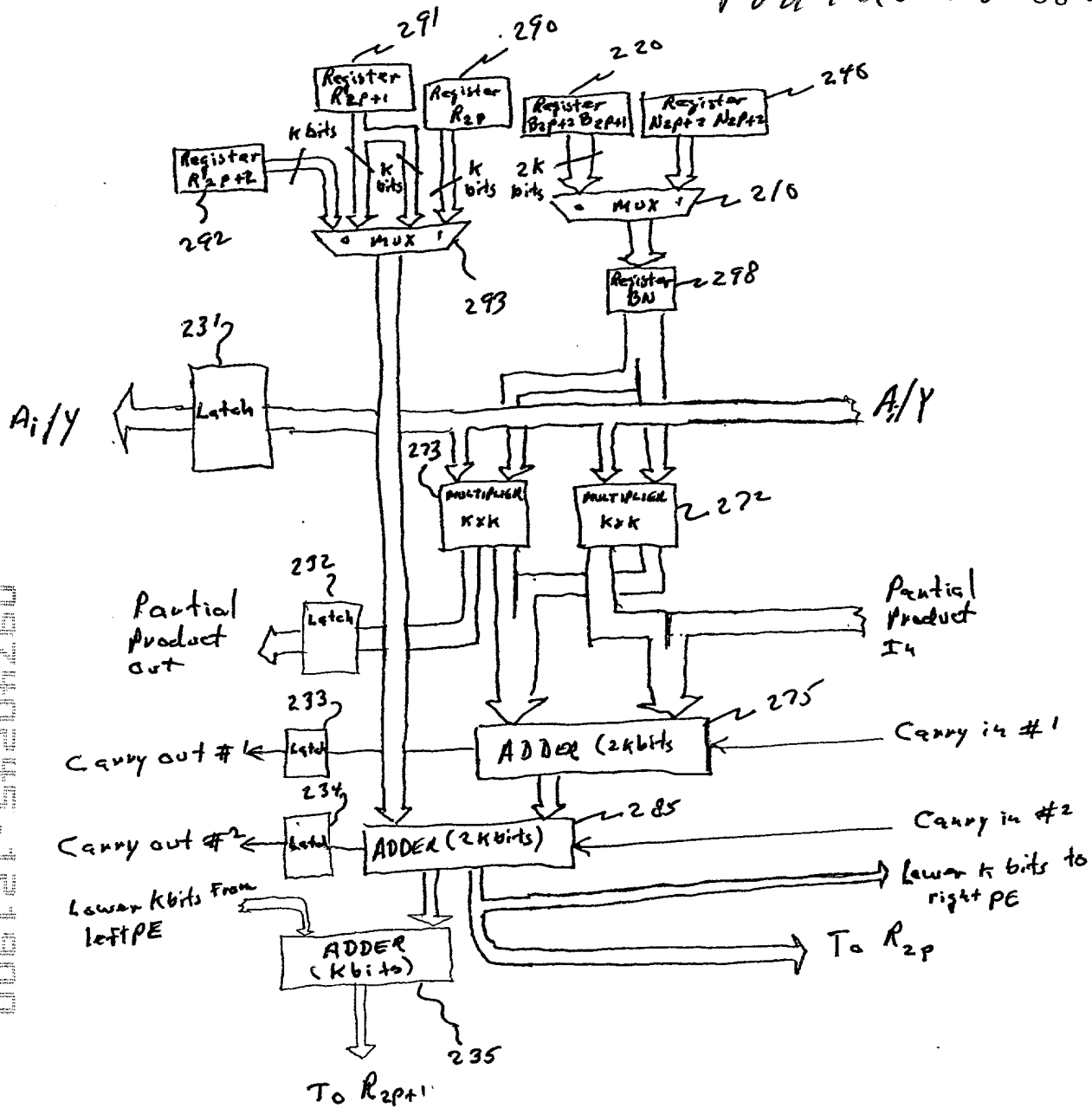


Figure 10

[illegible]

14/28

Pou 92000 028451

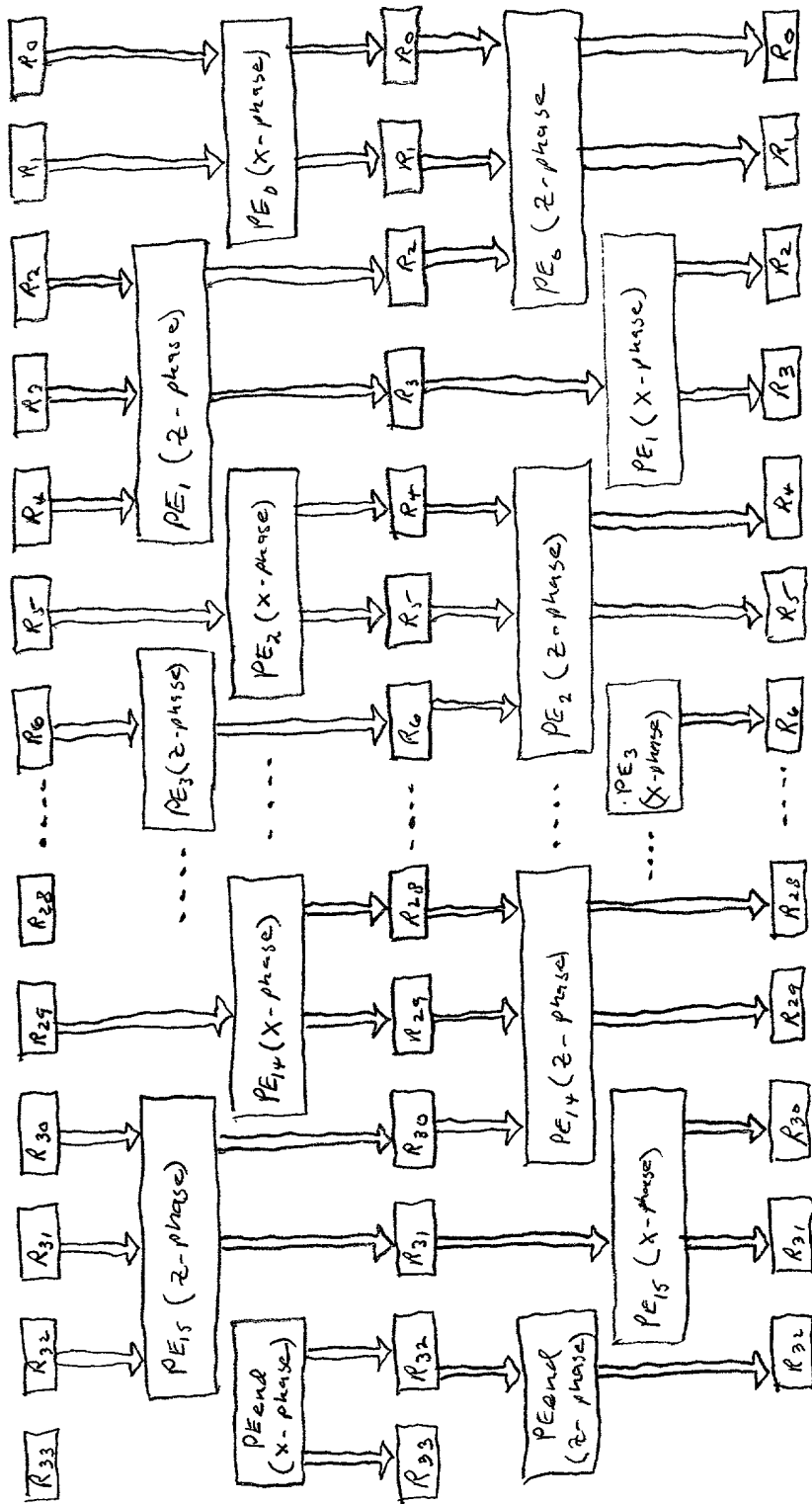


Figure 12

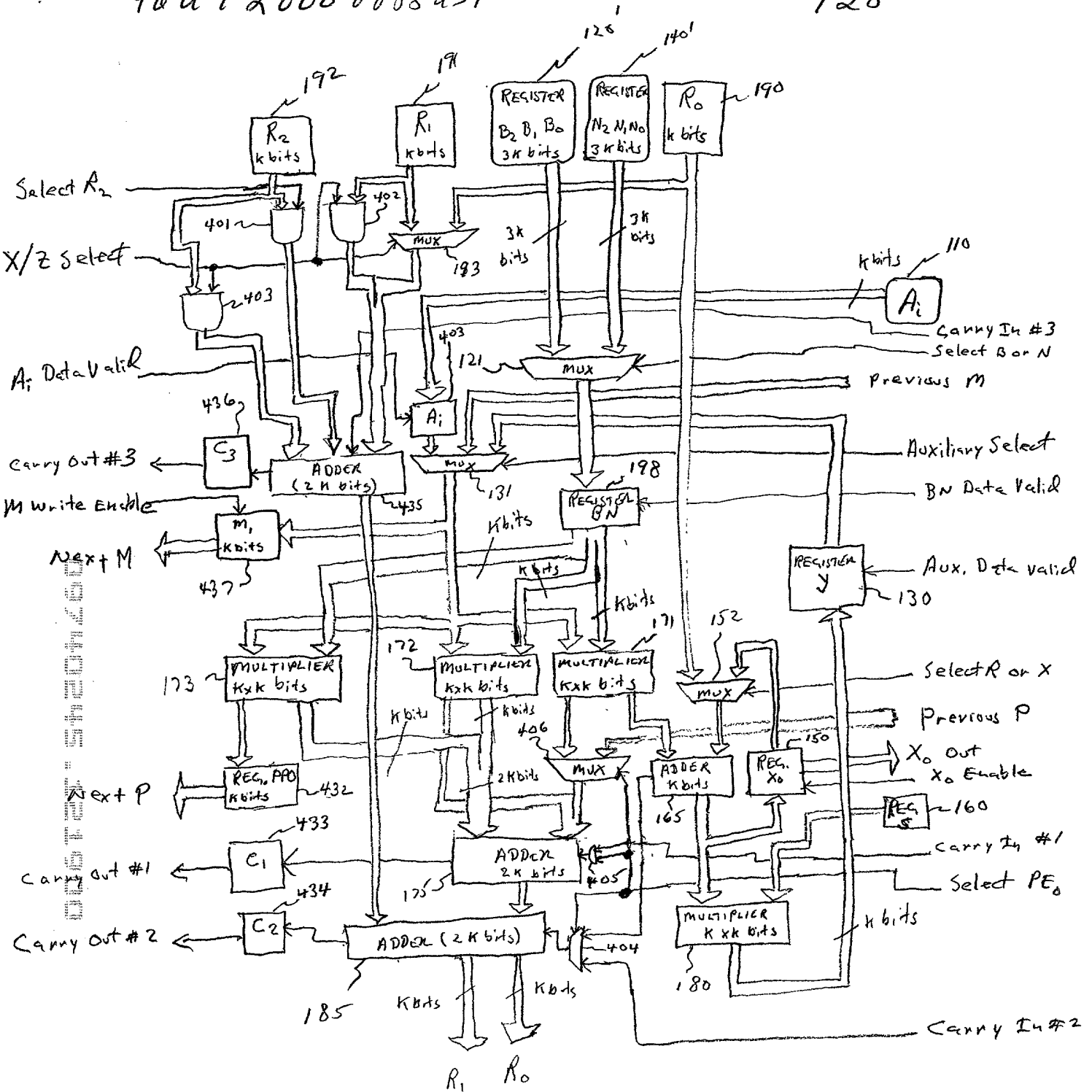


Figure 13

16/28

POU 92000 to 88451

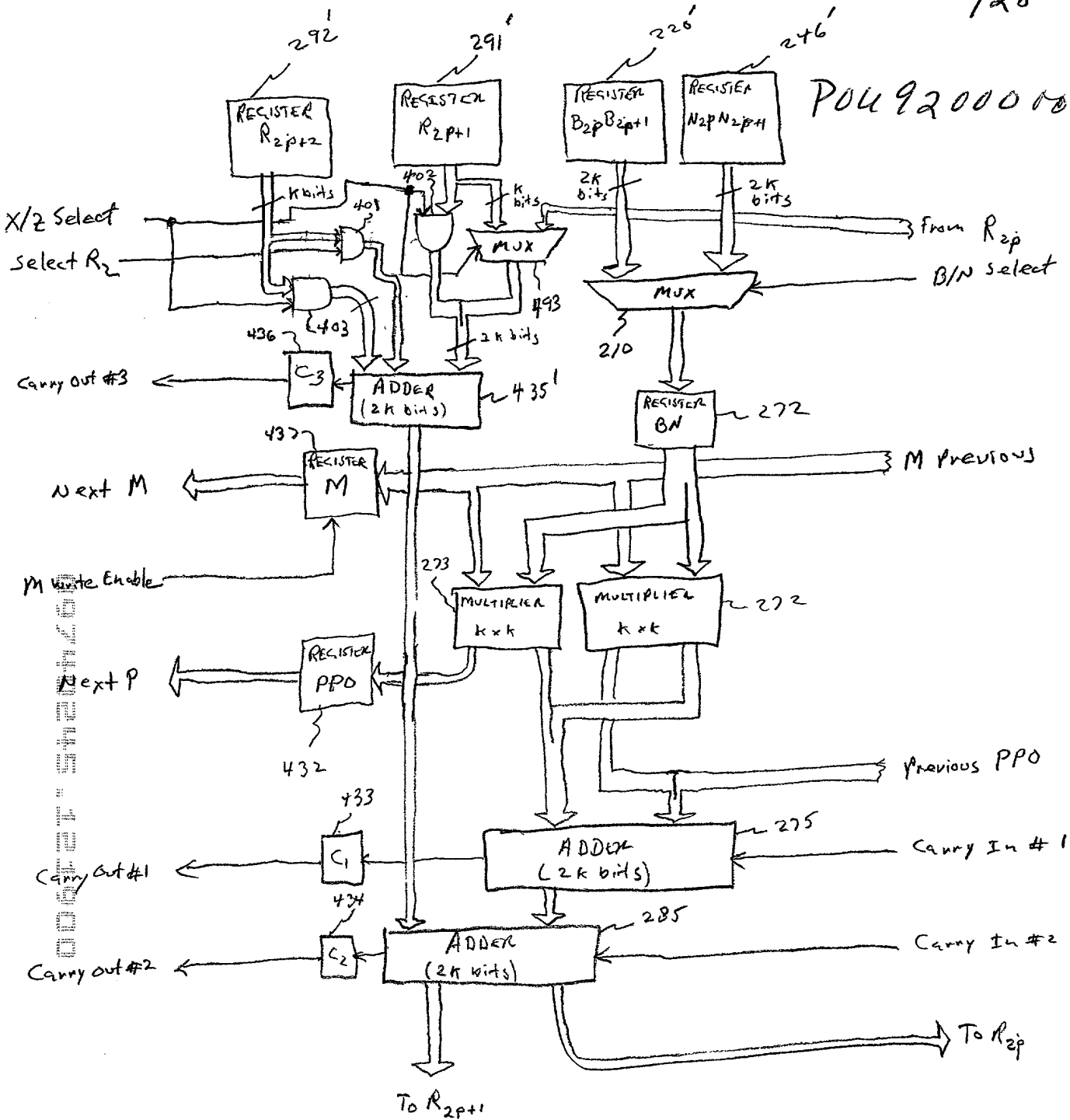


Figure 14

17/28

P0492000 0088451

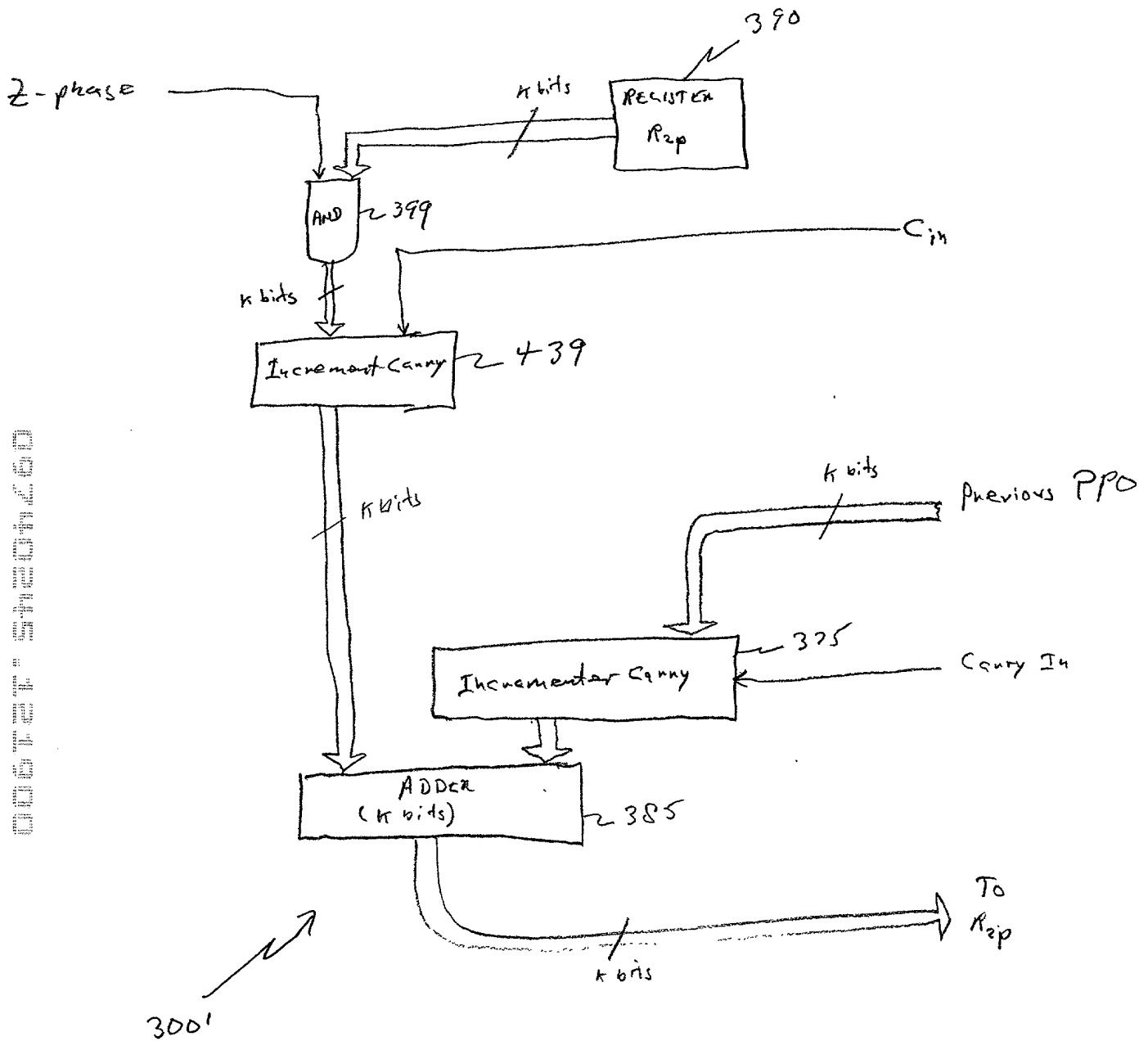


Figure 15

18/28

P0492000 0088451

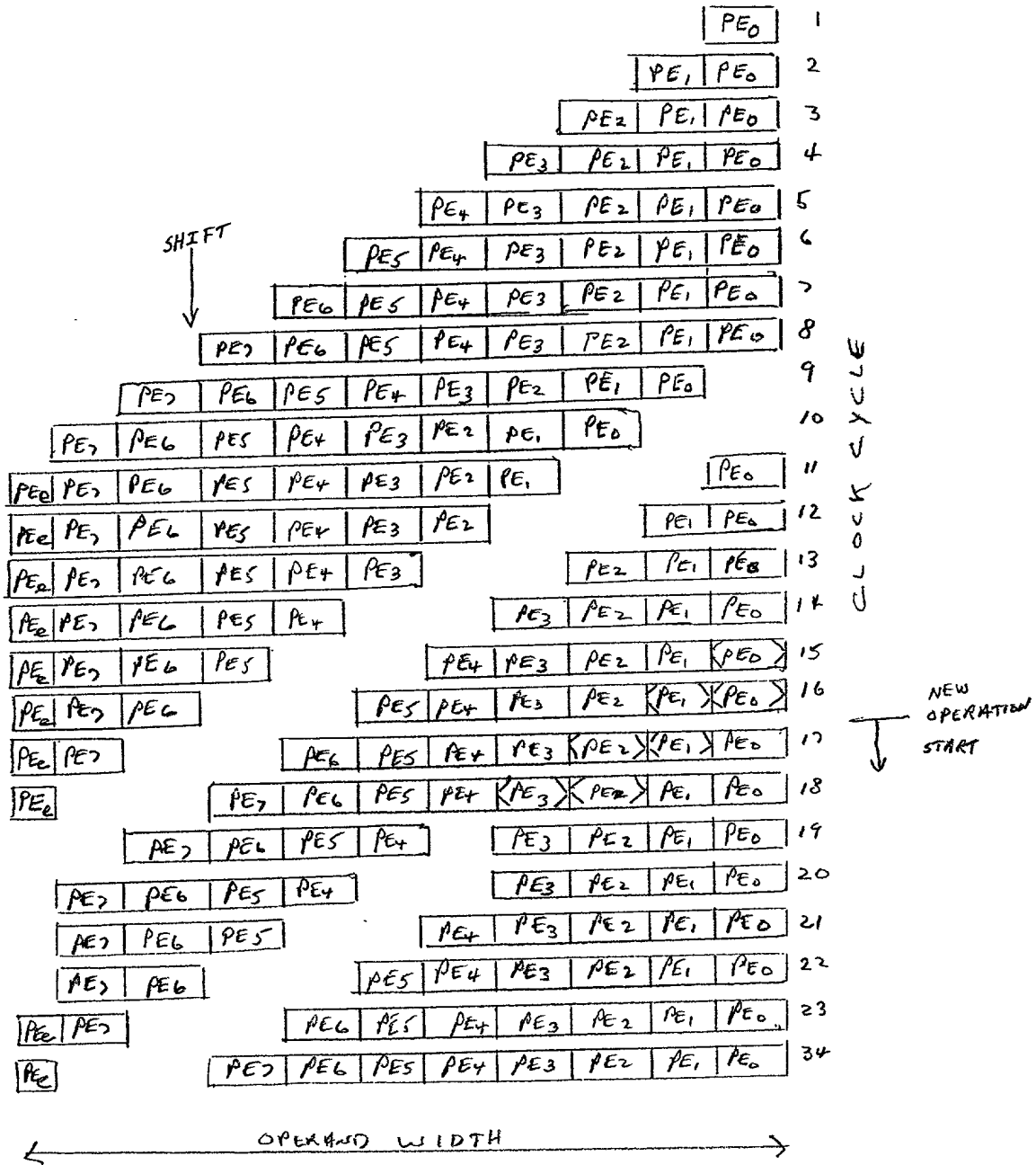


Figure 16

19/28

P0492000088US1

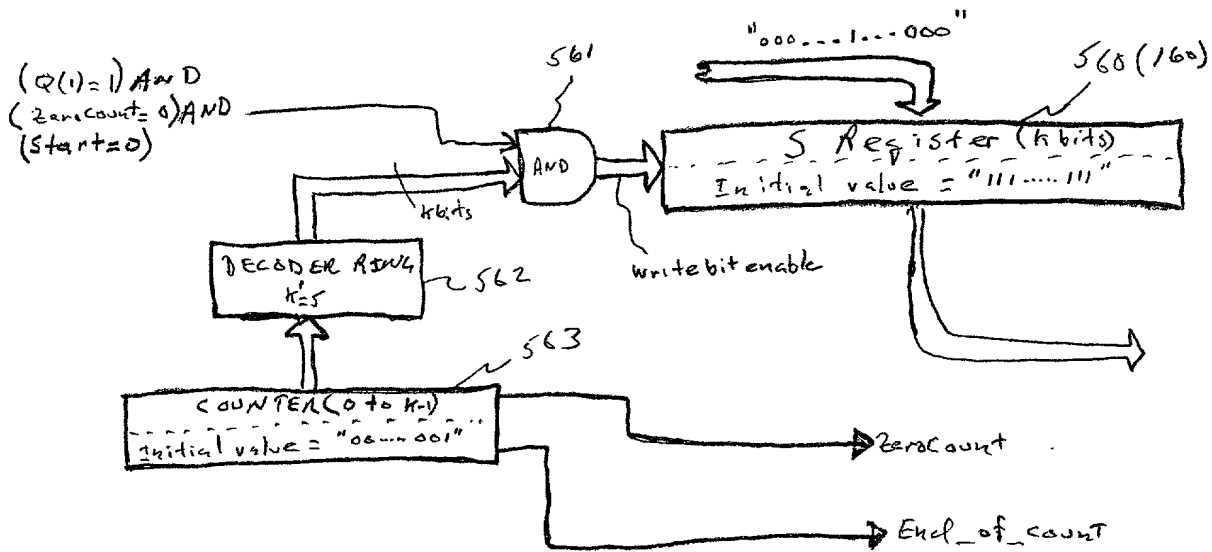
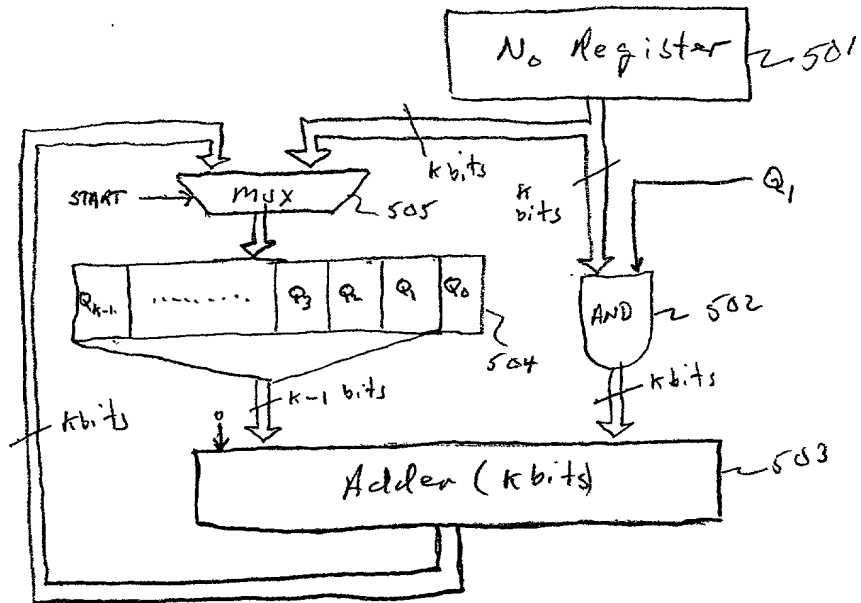


Figure 17

[illegible]

INPUT A, $E = \sum_{j=0}^t e_j 2^j$

$$C = 2^{2^{m-1}k} \bmod N$$
$$z_0 = f(A, c)$$
$$z_0 = f(A, c)$$

$$i = 1$$

$$z = f(z, z)$$

```

graph TD
    A[ ] --> B{ }
    B -- "Yes" --> C[ ]
    B -- "No" --> D[ ]
    style A fill:none,stroke:none
    style C fill:none,stroke:none
    style D fill:none,stroke:none
    
```

```

graph TD
    A[ ] --> B{ }
    B -- "Yes" --> C[ ]
    B -- "No" --> D[ ]
    style A fill:none,stroke:none
    style C fill:none,stroke:none
    style D fill:none,stroke:none
    
```

```

graph TD
    A[ ] --> B{ }
    B -- "Yes" --> C[ ]
    B -- "No" --> D[ ]
    style A fill:none,stroke:none
    style C fill:none,stroke:none
    style D fill:none,stroke:none
    
```

Yes

$$z = f(z, z_0)$$
$$i = i + 1$$

Is $i > t$?

Is $i > t$?

Is $i > t$?

$$z = f(1, z)$$

Figure 18

21/28

P0492000088451

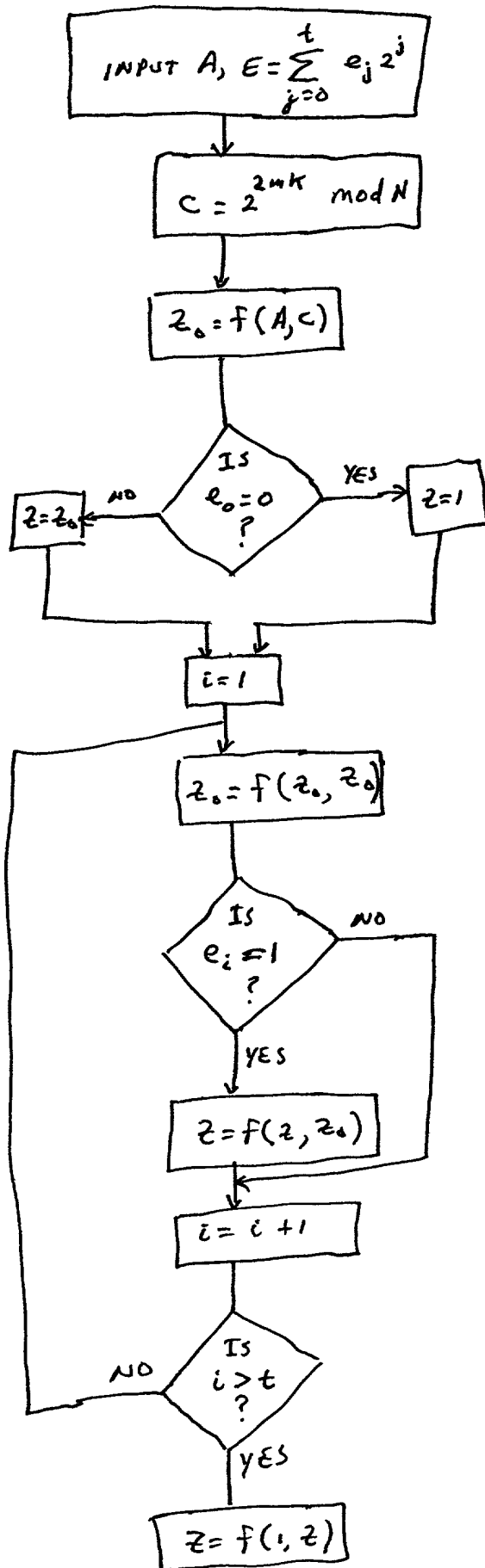


Figure 19

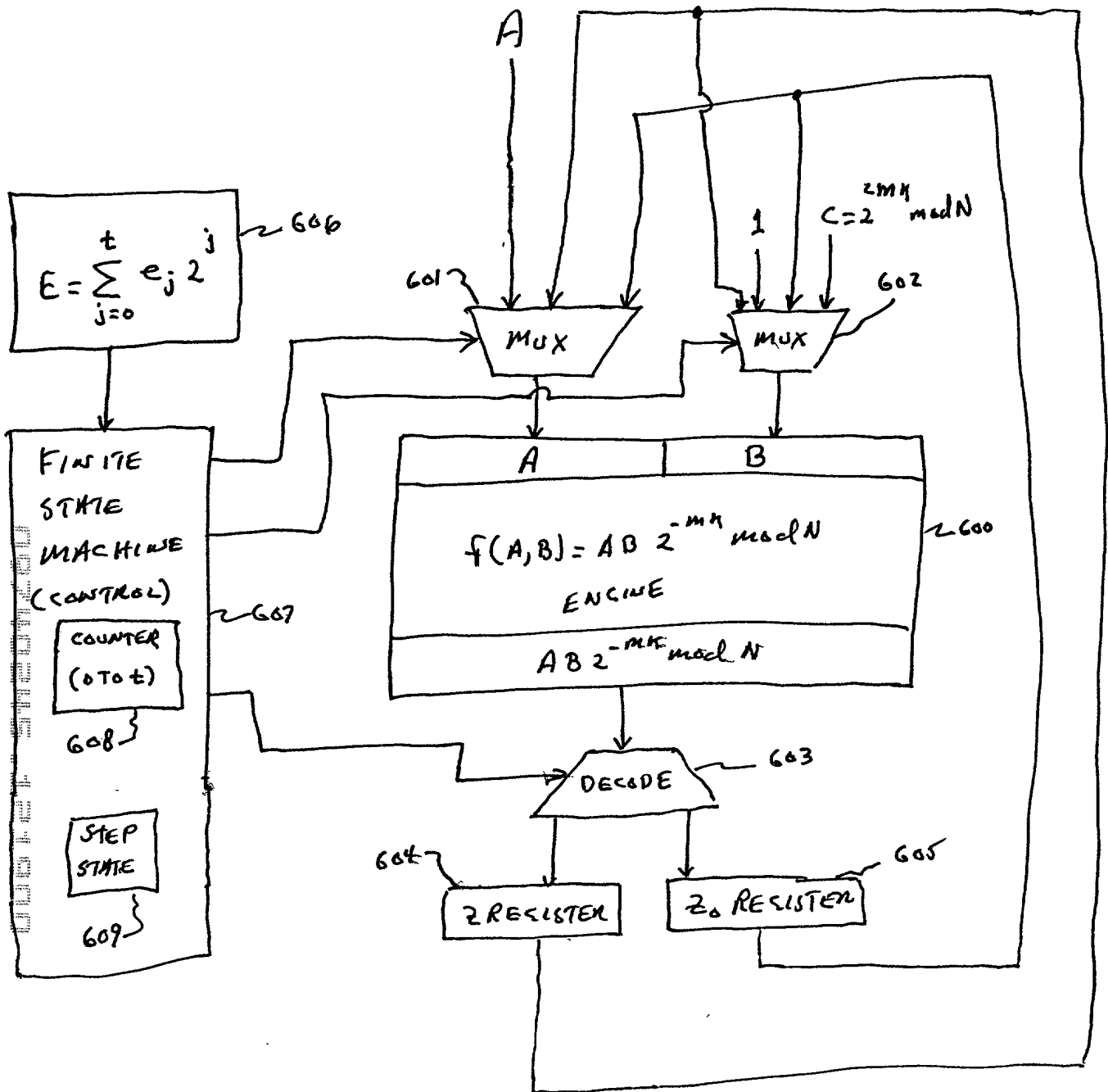


Figure 20

23/28 P0492000 0088451

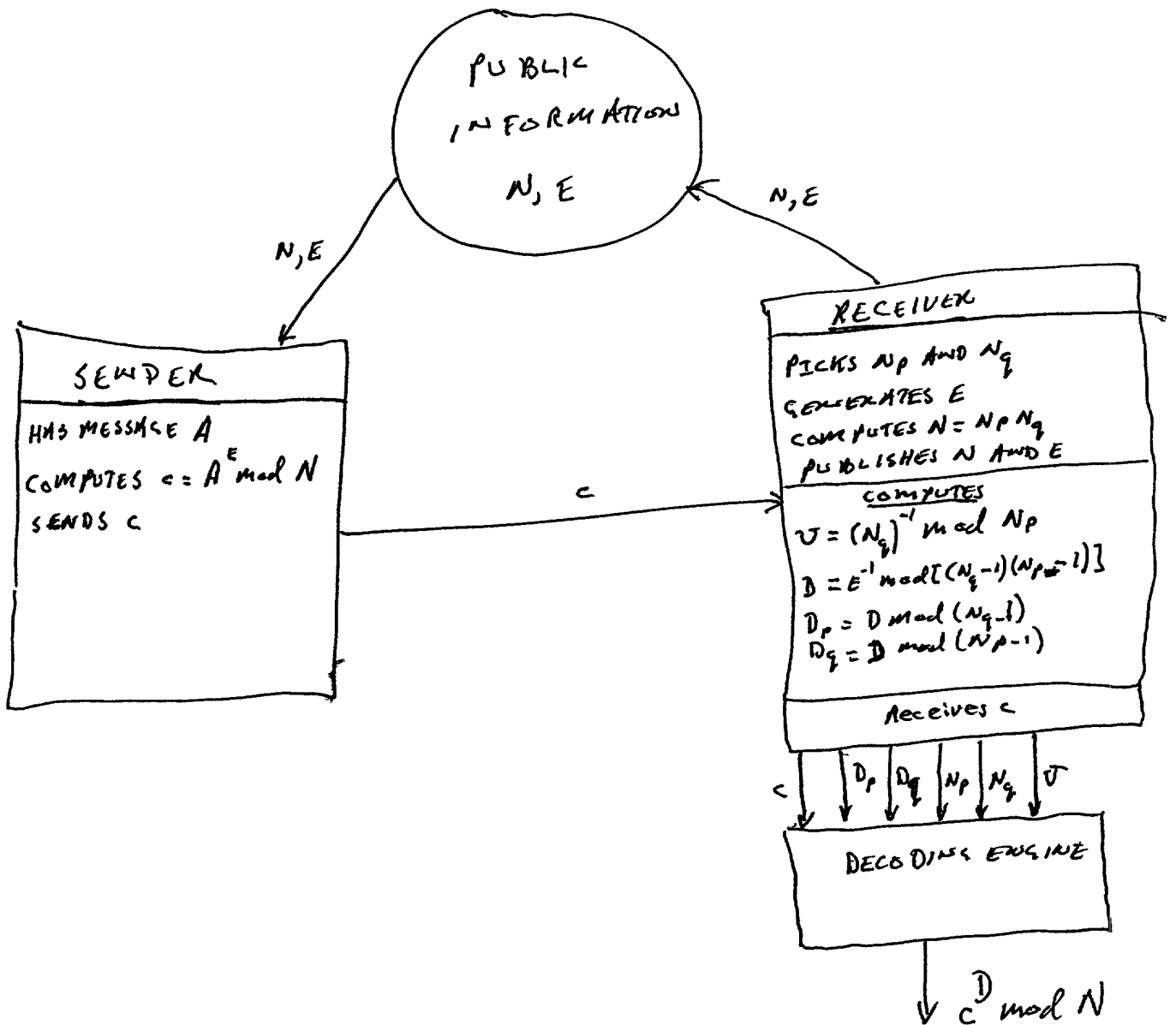


Figure 21

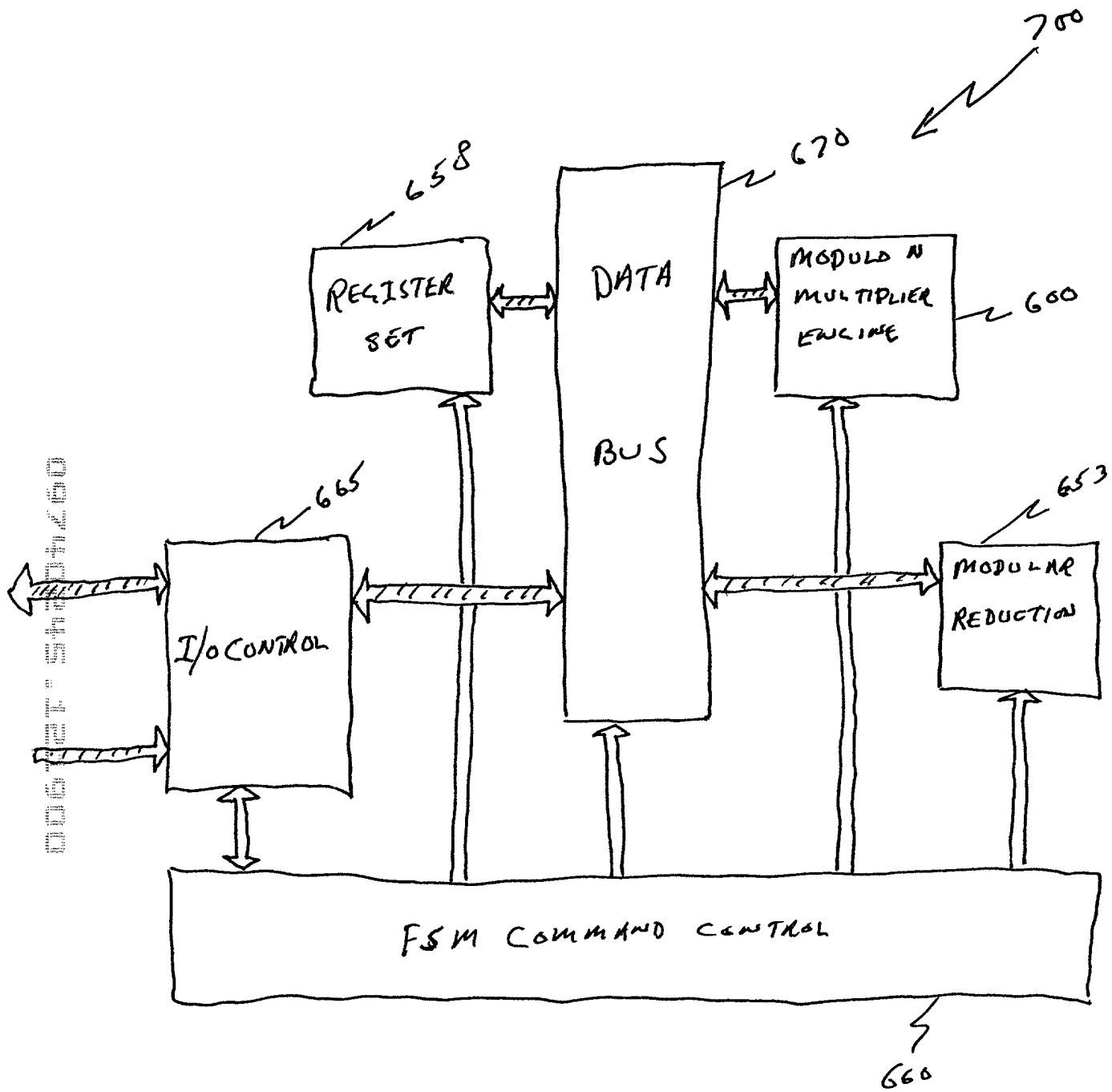


Figure 22

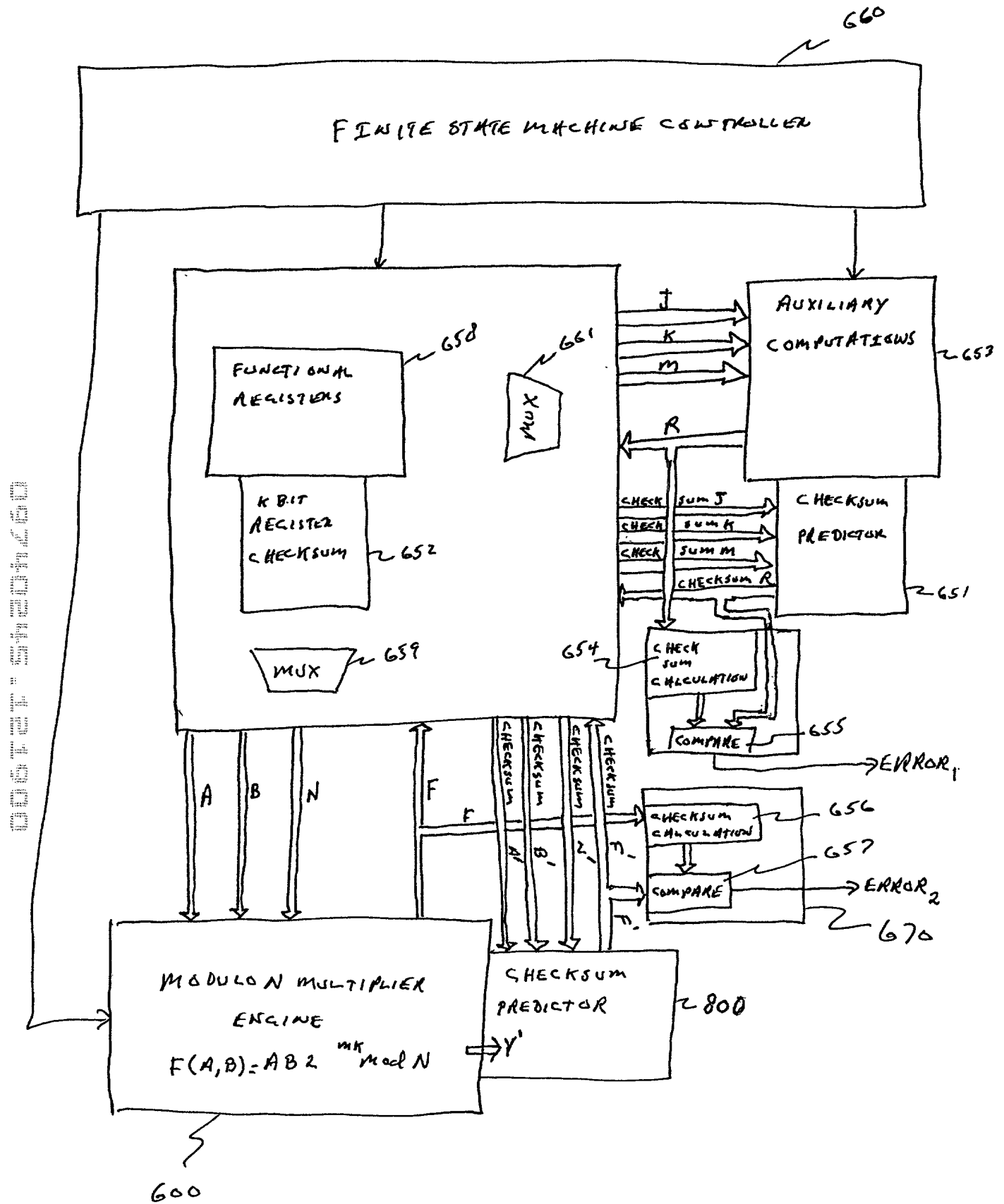
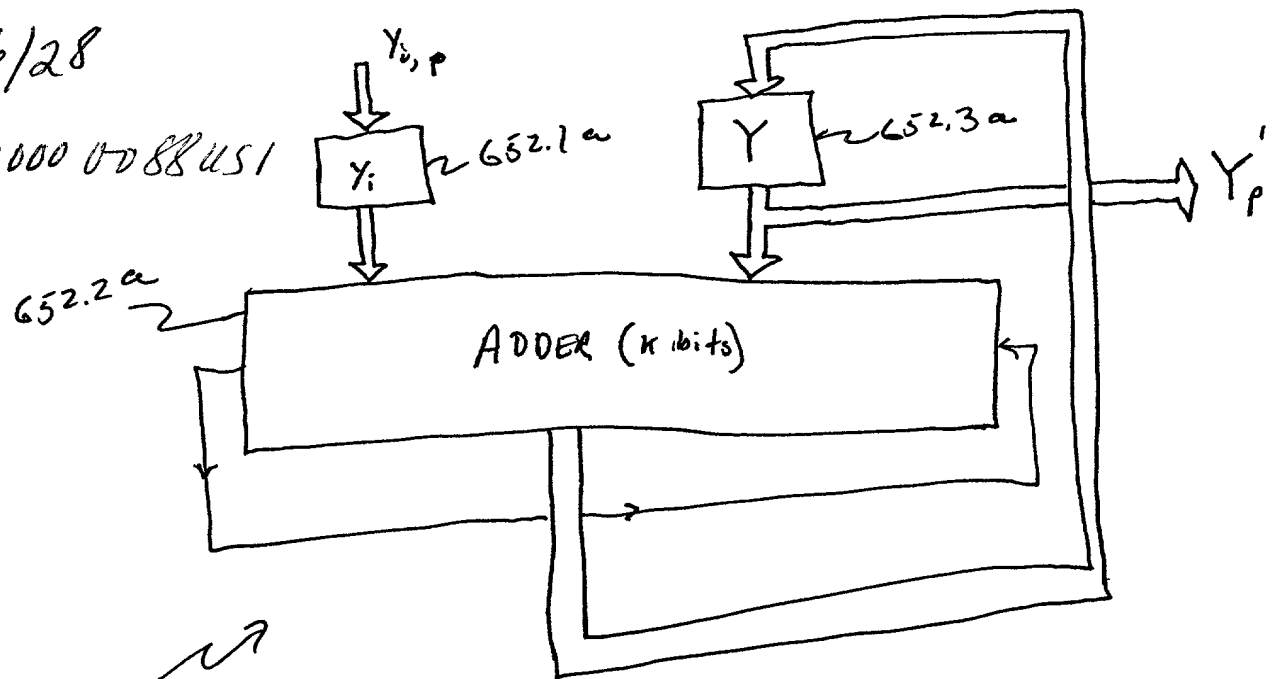


Figure 23

26/28

POU 92000 0088451



652a

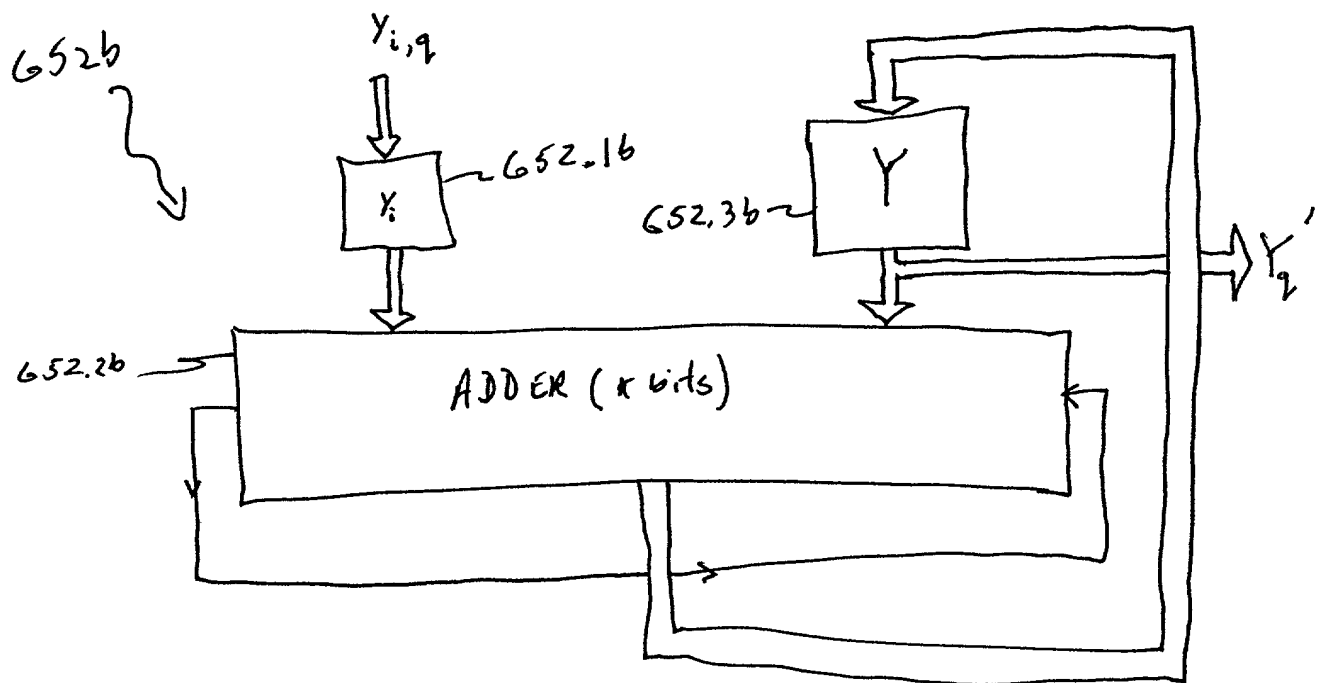


Figure 24

27/28 P0492000 v088451

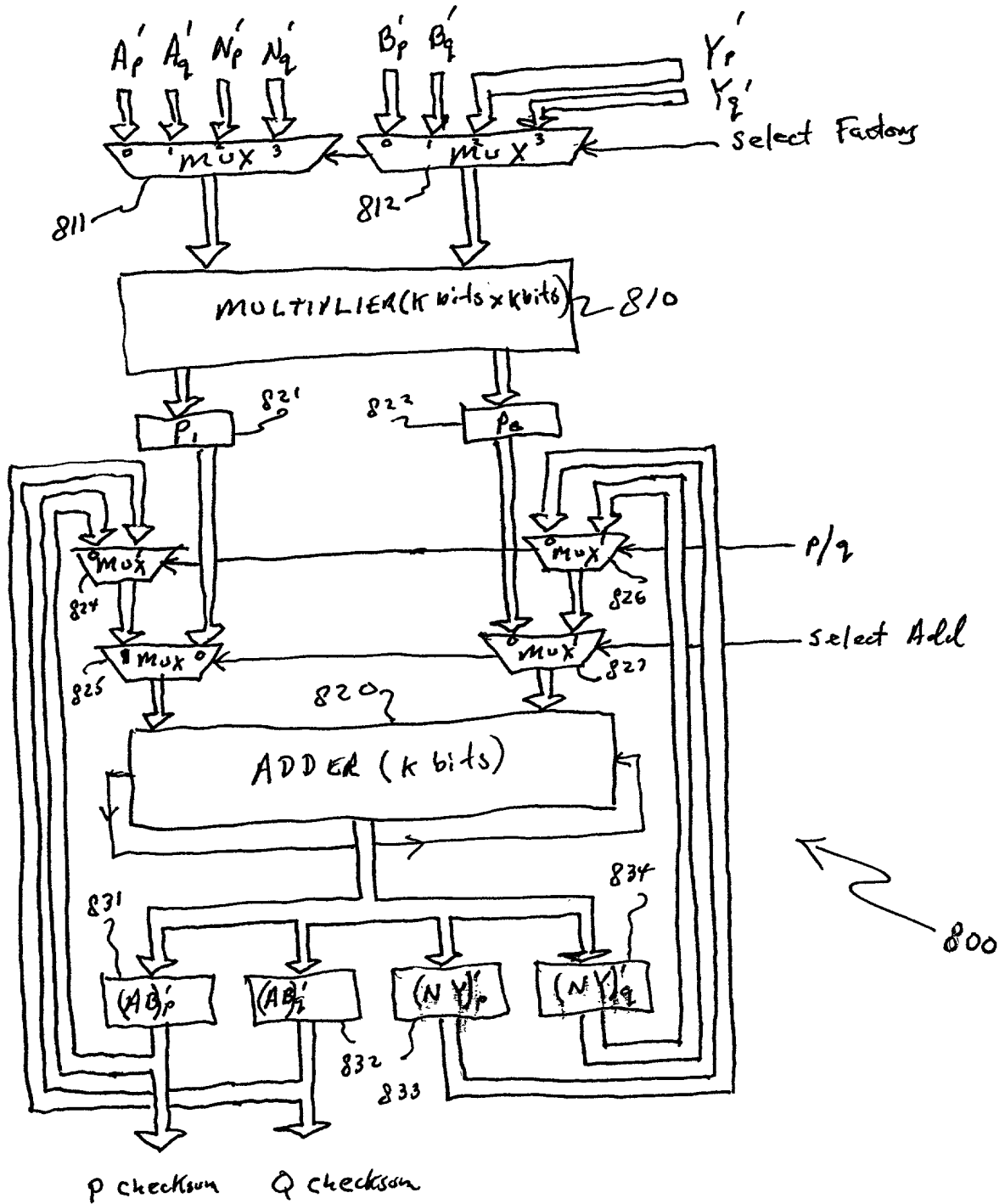


Figure 25

